Colloquium: Three Research Challenges from Claude Shannon

Joachim Rosenthal
University of Zürich
Mathematics Institute
8057 Zürich, Switzerland

In 1948/1949 Claude Shannon wrote two papers [Sha48,Sha49] which became the foundation of modern information theory. The papers showed that information can be compressed up to the 'entropy', that data can be transmitted error free at a rate below the capacity and that there exist provable secure cryptographic systems. These were all fundamental theoretical result. The challenge remained to build practical systems which came close to the theoretical optimal systems predicted by Shannon.

In this overview talk we will explain how the first two challenges concerning coding theory have resulted in practical solutions which are very close to optimal. Then we explain why the gap between the practical implementation of cryptographic protocols with the theoretical result of Shannon is largest.

References

[1] C.E. Shannon, *A mathematical theory of communication*, Bell Syst. Tech. J. **27** (1948), 379–423 and 623–656.

[2] C. E. Shannon, *Communication theory of secrecy systems*, Bell System Tech. J. **28** (1949), 656–715.